SafePatch
Installation Procedure

Introduction

SafePatch provides automated analysis of network-based computer systems to determine the status of security patches. SafePatch determines what patches are installed on a system and identifies those patches that need to be installed. Additionally, SafePatch can distribute identifiable patches to a remote system to be either automatically or manually installed.

Components

SafePatch is comprised of the following components:

SafePatch Server: A centralized server that schedules and controls the evaluation of remote systems. The Server may be executed from a non-privileged account.

SafePatch Agent: A remote system intended to be evaluated by the SafePatch Server. The Agent must be run from the root account.

SafePatch Databases: The following databases reside on a SafePatch Server.

> **Raw Database (RAWDB):** Contains raw patch files that have been collected from a vendor's ftp sites.
>
> **Patch Specification Database (PSDB):** Contains a set of vendor-neutral patch specification files. A specification file is generated for each raw patch file located within the RAWDB. The PSDB also contains a set of operating system specific baseline files. These files contain information associated with a pristine version of the operating system and are used during the evaluation process. One baseline file exists for each of the operating systems supported by SafePatch.

Java Runtime Environment (JRE) and the Java Cryptography Extension (JCE): These components are distributed with SafePatch and are self-contained within the SafePatch directory structure. By installing SafePatch, you agree to the licensing terms stated in the Sun license files found under the *"java/jre"* and *"java/jce"* sub-directories of SafePatch.

Hardware and Software Requirements

SafePatch Server:

Hardware:

- Minimum Memory: 128 MB RAM
- Minimum Disk Space: 8 GB

  Note: SafePatch, and the associated Java components, account for approximately 60 MB of the required disk space. The remaining disk space is reserved for those files that comprise the RAWDB and PSDB.

Software:

- Sun Solaris 2.5.1, 2.6, 2.7 or 2.8[1]
- DES cryptography software.
  (You can obtain DES from various sites such as ftp://ftp.psy.uq.oz.au/pub/Crypto/DES. Follow the README instructions for downloading, unzipping and using this software.)

SafePatch Agent:

Hardware:

- Minimum Memory: 64 MB RAM
- Minimum Disk Space: 50 MB for the Agent software
  50 MB for the patch download directory.
  (By default, the download directory is located in `/var/tmp/SafePatch`.)

Software:

- Sun Solaris 2.5.1, 2.6, 2.7 or 2.8 or Red Hat Linux 6.0, 6.1, 6.2, 7.1 or 7.2[2]
- DES cryptography software.
  (You can obtain DES from various ftp sites such as ftp://ftp.psy.uq.oz.au/pub/Crypto/DES. Follow the README instructions for downloading, unzipping and using this software.)

[1] The SafePatch Server is only officially supported on Solaris 2.7 and 2.8, but it has been successfully run on Solaris 2.5.1 and 2.6.

[2] SafePatch is configured to support agents on all of these platforms, but testing and official support for Solaris 2.5.1 and Red Hat Linux 6.0 and 6.1 has been dropped.

Acquiring the SafePatch Software

The SafePatch software can be acquired from http://ciac.llnl.gov/cstc/safepatch/safepatch.html. The software is distributed as a tar file containing a set of DES-encrypted tar files (one for the SafePatch Server and one for each OS specific version of the SafePatch Agent).

Once you have acquired the SafePatch software, you must register it at http://ciac.llnl.gov/cstc/safepatch/register.html. After the information you submit has been verified, you will receive a DES key to unlock the distribution files.

Installing the SafePatch Server

The following procedure can be used to install the SafePatch Server. By default, the Server distribution contains the Agent software and will be automatically installed on the Server host. Therefore, once you complete the installation of the Server software, you may elect to start the Agent.

Though you may utilize a non-root account for installing the Server, you must be root to execute the `setup` script detailed below.

1. If you have a previous version of SafePatch running, stop it before proceeding. First exit the graphical user interface if it is running. You can the stop the SafePatch Server and SafePatch Agent daemon processes by running the following scripts from the installation directory of the old version[3].

   To stop the SafePatch Server:
   ```
   > binm/StopJCS
   > binm/StopJobController
   ```

   If the SafePatch Agent is running on this computer:
   ```
   > binr/agent/StopAgent
   > binr/agent/StopRMIRegistry
   ```

2. Untar the file. Once the files have been extracted from the tar file, you may elect to delete the original distribution file.

[3] You can determine the installation directory by listing the /etc/safepatch.conf file using the following command:

> **`cat /etc/safepatch.conf`**

The installation directory is specified by the parameter **INSTALLDIR**.

```
> tar xvf SafePatch-X.Y.tar
> rm SafePatch-X.Y.tar
```
Where X.Y is the latest SafePatch version.

3. Decrypt the encrypted tar file by following the instructions included with your DES software. A typical command might be:

```
>./des -d -k "des-key" < SafePatch-X.Y-sol.tar.Z.des > [anyname].tar.Z
```

4. Once the file has been successfully decrypted, you may elect to delete the DES encrypted file.

```
> rm SafePatch-X.Y-sol.tar.Z.des
```

5. Uncompress and untar the file. A SafePatch directory will be created containing all relevant files. Once the files are unpacked and extracted, you may compress or delete the tar file.

```
> uncompress [anyname].tar.Z
> tar xvf [anyname].tar
```

6. Using the root account, generate a system configuration file by executing the commands below. Information entered during the `setup` procedure will be used to create the configuration file `/etc/safepatch.conf`. Entering a return at any prompt will set the default data (specified in brackets).

```
> cd SafePatch-X.Y
>./setup
```

If you have a previous version of SafePatch installed you will be asked the following two questions:

Do you want to use existing vendor server & target host information from the previous installation ([y]/n)?

[Answer yes, if you want to copy over host information from the old installation. No, if you want to recreate the host information from scratch. If you answer yes to this question, you must answer yes to copying keys for the server and all the agent installations.]

Do you want to use existing keys from the previous installation ([y]/n)?

[You must answer yes to this question, if you answered yes to the previous question. Answering yes to this questing copies the keys for the agent.]

Next the following information will be displayed:

```
Hostname:           [yourHost]
Directory:          [SafePatch-X.Y]
Configuration:      [/etc/safepatch.conf]
```

After the above information is displayed, the script will prompt for the following information.

User name under which SafePatch will run?

[Used to set the ownership of installed files. The specified account must exist.]

If you have installed a previous version of SafePatch you are done with setup. If this is a first time install, you will be asked the following additional questions:

Location of the patch download directory [/var/tmp/SafePatch]?

[Caution: Do not specify a directory whose files get deleted during boot (i.e., /tmp).]

Do you wish to maintain the ability to backout those patches that are installed during the automated patch installation process ([y]/n)?

If the answer to the this question is affirmed, the following question will be asked

Save Backout data to a directory other than the package database ([y]/n)?

If the answer to this question is affirmed, the following question will be asked

Enter absolute path of the directory to save backout data:

Location of the Raw Patch directory ==> [SafePatch-X.Y/RAWDB]

[Ensure partition contains 5GB of available disk space.]

Location of the Patch Specification directory ==> [SafePatch-X.Y/PSDB]

[Ensure partition contains 1GB of available disk space.]

Extracting Baseline patches …
Creating Diffie-Hellman Key for Agent …
Creating Diffie-Hellman Key for Command Center …

SafePatch provides the ability to encrypt data transferred among remote systems. For this reason, a pair of Diffie-Hellman keys are generated during the `setup` procedure. The Diffie-Hellman key pair for the server resides in the directory `SafePatch-X.Y/binm/D/CERTINFO` and are named `crt_SafePatch.pub` and `crt_SafePatch.prv`. The Diffie-Hellman key pair for an Agent is stored in the directory `SafePatch-X.Y/binr/CERTINFO` and are named `crt_[Hostname].pub` and `crt_[Hostname].prv`.

7. The SafePatch Server can be started by executing the below script. This script will start the interactive GUI and, if necessary, two Job Controller related daemon processes.

   > binm/SafePatch

   (Refer to the SafePatch User Manual for instructions on how to configure the Server.)

8. At this point, the installation of the SafePatch Server is complete. However, as previously mentioned, you may elect to start a SafePatch Agent on the Server

host. This is accomplished by executing the below script from the top-level SafePatch directory and must be executed under the root account. The script will start two daemon processes; the SafePatch Agent and Java's Remote Method Invocation (RMI) Registry.

```
> binr/agent/StartAgent
```

9. If you elect to activate the Agent on the Server host, you may wish to copy the file `util/SafePatchAgent` into one of your `/etc/rc?.d` directories. This will ensure the Agent is started each time your system is rebooted. You should review this file for correctness prior to moving it into a system directory.

   Example: `cp util/SafePatchAgent /etc/rc2.d/S97SafePatchAgent`

Installing a SafePatch Agent

The following procedure can be used to install the SafePatch Agent software. It is assumed that you have already acquired the DES key. Though you may utilize a non-root account for installing the SafePatch Agent, you must be root to execute the `setup` script detailed below.

1. If you have a previous version of the SafePatch Agent running, stop it before proceeding. You can the stop the SafePatch Agent processes by running the following scripts from the installation directory of the old version[4].

   ```
   > binr/agent/StopAgent
   > binr/agent/StopRMIRegistry
   ```

2. Decrypt the encrypted tar file by following the instructions included with your DES software. A typical command might be:

   ```
   >./des -d -k "des-key" < SafePatch-Agent-X.Y-OS.tar.Z.des > [anyname].tar.Z
   ```

   Where X.Y is the latest SafePatch version and OS is either sol if you're installing on a Sparc Solaris system or rhl if you're installing on an Intel Red Hat Linux system.

3. Once the file has been successfully decrypted, you may elect to delete the DES encrypted file.

   ```
   > rm SafePatch-Agent-X.Y-OS.tar.Z.des
   ```

---

[4] You can determine the installation directory by listing the /etc/safepatch.conf file using the following command:

> **`cat /etc/safepatch.conf`**

The installation directory is specified by the parameter **INSTALLDIR**.

4. At this point, you may wish to distribute the compressed tar file to each of the target hosts you intend to run a SafePatch Agent. The remaining commands would then need to be applied on each of the target hosts.

5. Uncompress and untar the file. A SafePatch directory will be created containing all relevant files. Once the files are unpacked and extracted, you may compress or delete the tar file.

```
> uncompress [anyname].tar.Z
> tar xvf [anyname].tar
```

6. Using the root account, generate a system configuration file by executing the commands below. Information entered during the `setup` procedure will be used to create the configuration file `/etc/safepatch.conf`.

```
> cd SafePatch-X.Y
>./setup
```

If you have a previous version of the SafePatch agent installed you will be asked the following question:

Do you want to use existing keys from the previous installation ([y]/n)?

[You must answer yes, if you answered yes when asked if you wanted to use existing vendor server & target host information during the SafePatch Server installation.]

Next the following information will be displayed:

```
Hostname:           [yourHost]
Directory:          [SafePatch-X.Y]
Configuration:      [/etc/safepatch.conf]
```

If you have installed a previous version of SafePatch you are done with setup. If this is a first time install, you will be asked the following additional questions. Entering a return at the prompt will set the default data (specified in brackets).

Location of the patch download directory [/var/tmp/SafePatch]?

[Caution: Do not specify a directory whose files get deleted during boot (i.e., /tmp).]

Do you wish to maintain the ability to backout those patches that are installed during the automated patch installation process ([y]/n)?

If the answer to the this question is affirmed, the following question will be asked

Save Backout data to a directory other than the package database ([y]/n)?

If the answer to this question is affirmed, the following question will be asked

Enter absolute path of the directory to save backout data:

Creating Diffie-Hellman Key for Agent …

SafePatch provides the ability to encrypt data transferred among remote systems. For this reason, a pair of Diffie-Hellman keys are generated during the `setup` procedure. The Diffie-Hellman key pair is stored in the directory `SafePatch-X.Y/binr/CERTINFO` and are named `crt_[Hostname].pub` and `crt_[Hostname].prv`.

After the Diffie-Hellman keys have been created, you will be prompted for a passphrase. The entered passphrase must be at least 8 characters and is used to encrypt the public key. The encrypted public key is stored in the file `SafePatch-X.Y/binr/CERTINFO/exchangeKey.pub`. When you configure an Agent from the Server, you will be prompted for the Agent's passphrase. The entered passphrase must be identical to the one specified during the Agent setup procedure described above. The passphrase encrypted public key adds an additional level of security by not transmitting the public key in clear text (Note: The exchange of public keys does not apply to the Agent residing on the Server).

7. Start the SafePatch Agent by executing the script below from the root account. The script will start two daemon processes; the SafePatch Agent and Java's Remote Method Invocation (RMI) Registry.

   `> binr/agent/StartAgent`

8. To ensure the Agent is started each time your system is rebooted, you may elect to move the file `util/SafePatchAgent` into one of your `/etc/rc?.d` directories. You should review the file for correctness prior to moving it into the system directory.

   Example for Solaris:
   `cp util/SafePatchAgent /etc/rc2.d/S97SafePatchAgent`

   Example for Red Hat Linux:
   `cp util/SafePatchAgent /etc/rc.d/rc3.d/S97SafePatchAgent`

Troubleshooting

1. Most installation errors result from an incorrect environment variable setting.

   Make sure your `PATH` environment variable includes `/bin`.

2. I cannot get the SafePatch Server GUI to display on a remote host through Ssh.

   If you utilize Ssh to remotely access the SafePatch Server GUI, you will need to disable X11 forwarding before the GUI will be displayed. This can be accomplished by the following command.

   `ssh -x <hostname>`

3. We recommend that you do not specify the `/tmp` directory as the download directory within the `setup` script. Contents within the `/tmp` directory are usually purged upon a reboot. Therefore, we recommend specifying a directory whose files will not be purged upon a reboot. The default directory (`/var/tmp/SafePatch`) is usually a good choice unless there does not exist enough disk space in the `/var` partition to store the patch distribution files.

4. An evaluation never completes and appears to be stuck within the "pending" queue.

   Due to inefficiency with the Java's Virtual Machine, a host running the SafePatch Agent must contain enough physical memory to hold the entire patch. In the event the host does not contain enough memory, the patch will not get downloaded to the target host and the job will never complete. By default, Java allocates a minimum of 4MB of memory and is allowed to grow to 16MB. In the event these values are inadequate, you may need to adjust the `-ms` and `-mx` command line parameters within the `StartAgent` script. Contact SafePatch@ciac.org for any assistance regarding this matter.

5. When I attempt to install patches I get the error message *"Unable to locate the unzip command"*. What does this mean?

   This message normally occurs under Solaris 2.6. Though Sun distributes patches in zip format, the `unzip` utility is not contained within the Solaris 2.6 operating system. To get around this limitation, we have included the `unzip` utility within the SafePatch distribution. It is located within the `util` subdirectory. Therefore, ensure the `util` directory is included within your PATH environment variable.

6. When I try to add a host, I get a message such as "`Connected. . . but could not find SafePatch agent.`" How do I fix this?

   This means one of two things: You need to restart the SafePatch agent on the client (you can do this by running the following commands from the SafePatch-Agent-x.y directory as root, where x.y is the version number and # is the shell prompt):

   ```
   # binr/agent/StopAgent
   # binr/agent/StopRMIRegistry
   # binr/agent/StartAgent
   ```

   Alternatively, it may mean that the client's `/etc/resolv.conf` is not set up properly (this is a problem if you use DNS on many Red Hat Linux systems). If the client machine name is `machine.example.org`, then make sure that the line

   ```
   search example.org
   ```

   appears in the `/etc/resolv.conf` on `machine.example.org` . In order to test, log into `machine.example.org` and issue the following commands.

   ```
   # ping -c 1 machine
   ```

```
# ping -c 1 machine.example.org
```

If you get a "unknown host" message, that means it's not configured correctly.

7. When I try to add a host, I get a message such as "`Unable to add host. . . key & passphrase have not been set or Agent is unable to read these files`." How do I fix this?

   If you're sure that the keys are set up correctly, check the `/etc/hosts` file. The machine name entry should be separate from the localhost entry. For example, if your machine name is `machine.example.org` and your IP address is 10.9.8.7, this `/etc/hosts` is incorrect:

   ```
   127.0.0.1  localhost.localdomain localhost machine.example.org machine
   ```

   This `/etc/hosts` is correct:

   ```
   127.0.0.1  localhost.localdomain localhost
   10.9.8.7   machine.example.org machine
   ```

8. I'm behind a firewall and cannot connect to the `safepatch.llnl.gov` ftp server. What do I need to do?

   This is a vendor specific question and is very hard for us to answer without specific information. Therefore, please contact your network administrator for assistance.

9. When all else fails, kill all SafePatch related processes on a host and restart the Server and/or the Agent software. The names of the SafePatch related processes are as follows:

   Server:

guilib.SafePatch	=> Interactive GUI process
SafePatchJCS	=> Daemon process
JobController	=> Daemon process

   Agent:

rmiregistry	=> Daemon process
agent.SolarisAgent	=> Daemon process

9. The patch installation process on Sun systems utilizes the `/tmp` partition. Failure to have adequate disk space within the `/tmp` partition may cause the patch installation process to fail. As a rule-of-thumb, the `/tmp` partition should contain enough disk space for holding 3 times the size of the largest patch.

Administrative Issues

If you desire to change the location of the SafePatch software, the Raw Database (RAWDB) directory, or the Patch Specification Database directory, you will need to re-execute the setup script located in the top-level SafePatch directory. This script will

update the SafePatch configuration file (`/etc/safepatch.conf`); and if the Raw Database directory or the Patch Specification directory has changed, it will prompt for their new location.

More Information

SafePatch, originally called SSDS, was changed to avoid confusion with other products and services with the SSDS name. SafePatch was developed by the Information, Operations and Assurance Center at Lawrence Livermore National Laboratory. SafePatch is sponsored by the Department of Energy's Security Affairs.

For more information, contact the SafePatch Project Leader at:

925-422-8193

e-mail: SafePatch@ciac.org

url: http://ciac.llnl.gov/cstc/safepatch/safepatch.html